WILLKIE FARR & GALLAGHER LLP
Benedict Y. Hur (SBN: 224018)
Simona Agnolucci (SBN: 246943)
Eduardo E. Santacana (SBN: 281668)
Tiffany Lin (SBN: 321472)
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599
bhur@willkie.com
sagnolucci@willkie.com
esantacana@willkie.com
tlin@willkie.com

Attorneys for
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

JONATHAN DIAZ and LEWIS BORNMANN, on behalf of themselves and all others similarly situated,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Case No. 5:21-cv-03080 NC

DEFENDANT GOOGLE LLC's NOTICE OF MOTION AND MOTION TO DISMISS THE FIRST AMENDED COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(1) AND 12(B)(6)

Judge: Hon. Nathanael Cousins
Court: Courtroom 5 – 4th Floor
Date: October 27, 2021
Time: 1:00 p.m.

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT, on October 27, 2021 at 1:00 p.m., the undersigned will appear before the Honorable Nathanael Cousins of the United States District Court for the Northern District of California at the San Jose Courthouse, Courtroom 5, 4th Floor, 280 South 1st Street, San Jose, CA 95113, and shall then and there present Defendant Google LLC ("Google")'s Motion to Dismiss the First Amended Complaint ("Motion").

Google brings this Motion under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure. Google will, and hereby does, move for an order dismissing the First Amended Complaint ("FAC") with prejudice because any additional amendment of the FAC would be futile. The Motion is based on this Notice of Motion and Motion, the following Memorandum of Points and Authorities, Google's Request for Judicial Notice, the Declaration of Tiffany Lin, and exhibits attached thereto, the pleadings and other papers on file in this action, any oral argument, and any other evidence that the Court may consider in hearing this Motion.

ISSUES PRESENTED

Whether Plaintiffs' FAC should be dismissed for lack of subject-matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) where Plaintiffs lack Article III standing; whether Plaintiffs' FAC should be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted; and whether the FAC should be dismissed with prejudice where any additional amendment would be futile.

WILLKIE FARR & GALLAGHER LLP

Date: August 25, 2021

By: *_/s/ Benedict Y. Hur_*
Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Tiffany Lin

Attorneys for Defendant
Google LLC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Authorities

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

In early 2020, as the world was grappling with the COVID-19 pandemic, Google and Apple, Inc. teamed up to develop technology to meet the needs of public health authorities to quickly and efficiently conduct digital contact tracing to slow the spread of COVID-19. The resulting Exposure Notification System ("EN System") was developed with robust privacy protections in place. Over the past year, the EN System has been used by millions of users and dozens of public health authorities around the world. Google and Apple made the technology available free of charge.

Apparently no good deed goes unpunished. Plaintiffs Jonathan Diaz and Lewis Bornmann do not allege that the EN System disclosed personally identifiable information ("PII") to *anyone*. Their claims instead hinge on an entirely hypothetical theory that unrelated apps engaged in an increasingly remote and malicious series of steps to attempt to learn something from crash-reporting logs. But they don't allege that any bad actor has gone to the lengths that would be necessary to decipher a user's identity, decipher the information logged by the EN System, and make guesses or inferences about the user's activity within the app. They merely allege it is theoretically possible that someone *could* have done that. This is thus a textbook case about a hypothetical risk of harm that is not, in any event, fairly traceable to Google's conduct.

Google moved to dismiss once already, and rather than oppose, Plaintiffs responded by amending their complaint. The First Amended Complaint ("FAC") adds many words but still lacks factual allegations showing that an individual's use of the EN System was ever used to identify an individual and their COVID-19 test result, and the explanations for how that might be possible are convoluted and theoretical.

Google now moves to dismiss Plaintiffs' FAC with prejudice because: (1) Plaintiffs have failed to establish Article III standing; (2) Plaintiffs cannot state a claim for privacy violations under California common law, the California Constitution, or the California Confidentiality of Medical Information Act ("CMIA"); and (3) any additional amendment of the FAC would be futile.

II. BACKGROUND

A. Relevant Procedural History

Plaintiffs filed a Class Action Complaint on April 27, 2021. ECF 1. Google filed a Motion to Dismiss the Complaint on June 29, 2021. ECF 18. In lieu of opposing Google's Motion to Dismiss, Plaintiffs filed a FAC on July 20, 2021. ECF 24. The FAC alleges the following claims: (1) public disclosure of private facts; (2) intrusion upon seclusion; (3) violation of Article I, Section 1 of the California Constitution; and (4) violation of the CMIA.

B. Relevant Factual Background

1. Exposure Notification System

In early 2020, Google and Apple developed the Exposure Notification System that uses applications on mobile devices to aid in digital contact tracing efforts.[1] FAC ¶¶ 12–17. The goal of the EN System is to assist public health authorities in their efforts to fight COVID-19 by enabling exposure notifications in a privacy-preserving manner.[2] Google and Apple have released software tools called Application Programming Interfaces ("APIs") that enable public health authorities to build mobile applications to help with COVID-19 contact tracing efforts across Android and iOS devices in a privacy-protective way.[3] The EN System can be used only to support approved contact tracing apps of authorized public health authorities.[4] Some public health authorities have built apps that use the EN System, some use a template app developed and supported by Google, and other public health authorities offer contact tracing using the EN System without creating an app (CA Notify on iOS devices is one example).[5] FAC ¶¶ 16–21. In all cases, in order to enable

---

[1] *See* Google's RJN Ex. 1, *Use the COVID-19 Exposure Notifications System on your Android phone*, Google Play Help, https://support.google.com/googleplay/answer/9888358?hl=en (last visited August 6, 2021); Google's RJN Ex. 2, *Exposure Notifications: Using technology to help public authorities fight COVID-19*, Google COVID-19 Information and Resources, https://web.archive.org/web/20201201225451/https://www.google.com/covid19/exposurenotifications/ (last visited August 6, 2021); Google's RJN Ex. 3, *Exposure Notifications: Frequently Asked Questions*, September 2020 v1.2, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf.

[2] *See* Google's RJN Ex. 3.

[3] *Id.*

[4] *Id.*

[5] *Id.*; Google's RJN Ex. 1.

the EN System, the user must activate exposure notifications and consent to the terms and conditions of their public health authority's contact-tracing app or services.[6] FAC ¶¶ 19–26. Google and Apple committed not to monetize the EN System, and to disable it on a regional basis when it is no longer needed.[7]

Once the EN System is enabled by the user, the user's device will periodically send out a beacon via Bluetooth that includes a Rolling Proximity Identifier ("RPI"): a string of random numbers that aren't tied to a user's identity and that changes every 15 to 20 minutes.[8] FAC ¶¶ 29–31. When two phones with the EN System enabled come into proximity of one another, they exchange their then-current RPIs, which are stored on the devices.[9] *Id.* ¶ 30. The devices also generate a Temporary Exposure Key ("TEK") that changes every 24 hours. *Id.* ¶¶ 27–28. Neither RPIs nor TEKs contain personal information. *Id.* ¶¶ 27, 29. RPIs and TEKs are stored on users' devices, and after 14 days they are deleted.[10]

If a user receives a positive COVID-19 test result, a local public health authority can provide the user with a verification code to report that test result in the health authority's app. *Id.* ¶ 38. After the test result is reported, the EN System enables the user to choose to upload the TEKs generated over the last 14 days on their device.[11] *Id.* Public health authorities designate a server to maintain a list of TEKs associated with users who have reported a positive test result.[12] Apps using the EN System periodically download and compare the list of TEKs of users who have reported a positive test result to the list of RPIs each user has come into contact with over the past 14 days. *Id.* ¶ 40. If the EN System determines that a user has come into contact with an RPI generated by a TEK associated with a user who reported a positive test result, the health authority's app can display an exposure notification to the potentially exposed user. *Id.* ¶ 42. The

---

[6] Google's RJN Ex. 4: *CA Notify: Apps on Google Play*, Google Play, https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenotifications (last visited August 6, 2021).
[7] Google's RJN Ex. 3.
[8] *Id.*
[9] *Id.*
[10] Google's RJN Ex. 4.
[11] *See also* Google's RJN Ex. 3.
[12] *Id.*

exposure notification alerts the potentially exposed user that they have recently come in contact with someone who has tested positive for COVID-19 and provides the health authority's guidance on next steps.[13] The EN System shares with the health authority the day the contact occurred, how long it lasted, the Bluetooth signal strength of that contact, and the type of report that confirmed the test result.[14] The EN System was designed so that users decide whether to share their COVID-19 diagnosis with their local public health authority, and they are not identified to other users.[15]

CA Notify is California's implementation of the EN System. The December 2020 CA Notify Privacy Policy provides that the following categories of de-identified data may be processed and collected by CA Notify: (1) Installing and deleting the app (Android only); (2) Enabling and disabling exposure notifications; (3) Receiving an exposure notification; (4) Entering a verification code to send anonymous keys; (5) Anonymous keys that have been voluntarily shared.[16] The policy states, "[t]he data may also be shared with local public health authorities and the University of California. This information will not include any personal or location information, nor can it be used to identify any system user."[17] The policy also provides that, though a user's identity is not shared, "[i]t is possible that someone who receives an exposure notice could guess the identity of the COVID-19 positive individual, if they had a limited number of contacts on a given day."[18]

2. Plaintiffs' Allegations

The FAC alleges[19] that the EN System produced three types of log entries in Android system logs meant for crash reporting: (1) the user's Bluetooth RPIs; (2) an "activity"[20] that starts

---

[13] Google's RJN Ex. 3.
[14] *Id.*
[15] *Id.*
[16] Google's RJN Ex. 5, *Privacy Policy*, CA Notify, https://covid19.ca.gov/notify-privacy/ (effective Dec. 10, 2020).
[17] *Id.*
[18] *Id.* Public health authorities that use Google's EN service must comply with the Google COVID-19 Exposure Notifications Service Additional Terms as well as Google's API Terms of Service. *Google COVID-19 Exposure Notifications Service Additional Terms* (May 4, 2020), https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf.
[19] As it must, Google treats the allegations of the FAC as true for purposes of this motion.
[20] Plaintiffs refer to an "activity" in the Android Operating System as "a discrete screen within the application." FAC ¶ 81.

when a user elects to report a positive COVID-19 test result named "ShareDiagnosisActivity"; and relatedly, (3) an entry reflecting that the user had taken steps to upload TEKs to the public health authority. FAC ¶¶ 57–59; 76–77; 84–88. Plaintiffs allege that Google, certain applications on Android devices, and third-party entities affiliated with those apps, have permission to access the crash-reporting logs. *Id.* ¶¶ 60–66. Plaintiffs also allege that Google, device manufacturers, and mobile network operators collect information from the crash-reporting logs. *Id.* ¶¶ 91–92. Finally, Plaintiffs allege that the entities with access to the crash-reporting logs can "associate the data that [the EN System] logs with the device owner's identity." *Id.* ¶ 98. Plaintiffs allege that users of Apple iPhone devices are also harmed because "the RPIs [the iPhone] transmits are being logged with identifying information by Android devices running [the EN System], from which it is communicated to Google and perhaps dozens of other third parties." *Id.* ¶ 114. Plaintiffs don't allege that anybody reviewed the log to determine whether a particular user reported a positive COVID-19 test result.

Furthermore, nothing in the FAC alleges that *any* facet of the EN System itself logs PII. It doesn't. The only piece of information logged by the EN System that Plaintiffs allege could be characterized as "identifying information" is a user's randomized MAC address. Though Plaintiffs acknowledge that MAC addresses are "string[s] of characters" that "are randomized before broadcast," Plaintiffs allege that "randomized MAC addresses can be associated with specific locations," FAC ¶ 103. But the lone 2017 study that Plaintiffs cite for this concept contains highly technical de-randomization techniques and, most importantly, appears to conclude that the main issue "is that the overwhelming majority of Android devices are not implementing the available randomization capabilities built into the Android OS."[21] This study is entirely inapplicable to the instant situation where Plaintiffs admit the EN System uses randomized MACs. FAC ¶ 34.

Because the EN System does not log PII, Plaintiffs allege instead that the same crash-reporting logs to which the EN System logs data may contain PII that was *included by others*

[21] FAC ¶ 103 n. 52. Plaintiffs also cite to two inapposite news articles that appear to conclude that MAC addresses that are *not* randomized or anonymized can be used by retail analytics providers to track devices, but anonymization or randomization of MAC addresses may prevent tracking and improve smartphone privacy. *See* FAC ¶ 194 n. 53.

against Google's guidance, and that yet another entity could then collect that data at exactly the right time and combine it to link a person's identity to their decision to report a positive COVID-19 test result. *See* FAC ¶¶ 74; 98–99; 104–10.

Plaintiffs allege that Named Plaintiffs Lewis Bornmann and Jonathan Diaz downloaded and activated the CA Notify app on Android devices in December 2020. *Id.* ¶¶ 124, 129. Plaintiffs do not allege whether Bornmann entered a positive test result into the CA Notify app, nor whether he interacted with the App in any way after installing and activating the app. *Id.* ¶¶ 124–28.

The FAC explains that Google began "rolling out patch fixes" to change the logging in late March 2021. *Id.* ¶ 117. Plaintiffs allege that the logging of RPIs, activity names that purportedly reflect a user making a report, and entries purportedly showing that a user had taken steps to upload TEKs to the public health authority by the EN System code occurred until at least April or May 2021. *Id.* ¶¶ 76–77; 86–88; 117–21. Plaintiffs do not allege that there is any present feature of the EN System that violates their rights. *Id.*

III. RULE 12(B)(1) MOTION TO DISMISS

A. Legal Standard

It is the plaintiff's burden to establish subject-matter jurisdiction.[22] *See Kingman Reef Atoll Inv., LLC v. United States*, 541 F.3d 1189, 1197 (9th Cir. 2008). "[L]ack of Article III standing requires dismissal for lack of subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1)." *Naruto v. Slater*, 888 F.3d 418, 425 n.7 (9th Cir. 2018). To establish Article III standing, the plaintiff must show: "(1) a concrete and particularized injury, that (2) is fairly traceable to the challenged conduct, and (3) is likely to be redressed by a favorable decision." *Virginia House of Delegates v. Bethune-Hill*, 139 S. Ct. 1945, 1950 (2019). The injury must be "(a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

"[S]tanding theories that require guesswork as to how independent decisionmakers will exercise their judgment" or "rest on speculation about the decisions of independent actors" do not

[22] Internal citations and quotation marks have been omitted and emphases added unless otherwise noted.

meet the "certainly impending" and "fairly traceable" requirements for Article III standing. *See Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 413 (2013).

C. Argument

1. Plaintiffs lack Article III standing.

Plaintiffs lack Article III standing because their alleged injury is not (1) concrete or particularized; (2) fairly traceable to the challenged conduct; or (3) would not be redressed by a favorable decision.

a. Plaintiffs' alleged injury is not concrete or particularized.

i. Plaintiffs' allegations rest upon a highly attenuated chain of possibilities.

Plaintiffs cannot show that they have suffered, or will imminently suffer, a concrete or particularized injury. Plaintiffs' argument rests on the highly speculative fear that, despite the temporary nature of the data logged into the crash-reporting log, the privacy-protective design of the TEKs and RPIs, the technical and standardized nature of the information logged about the EN System's operation, the limited access to the crash-reporting log and TEK list, the regeneration of random TEKs every 24 hours and random RPIs every 15 minutes, and the various privacy policies and protections in place, a bad actor could seek to collect and comb through this data at exactly the right moment and combine the non-PII contained in the crash-reporting logs in order to infer the identity of someone who reported a positive COVID-19 test result. *See* FAC ¶ 98.

Plaintiffs allege in conclusory fashion that "[t]he exposed [crash-reporting log] information is personally identifiable." FAC at 1. Plaintiffs rest their allegation on the assumptions that: (1) randomized MAC addresses are "identifying information"; (2) the information in the EN system is somehow "linked" to PII; and (3) a third party can view the information in the crash-reporting log at any moment. All of these assumptions are incorrect.

First, as described above, a randomized MAC address cannot be used to identify an individual, but only, after much work, potentially a specific location (but even that is highly unlikely). *See* FAC ¶ 103. Regardless, going through several hoops to convert a MAC address into a specific location is just the type of conjectural and speculative harm that falls short of establishing Article III standing. Plaintiffs do not point to a single instance, or even a whiff of

suspicion, that anyone has ever used a randomized MAC address in a crash-reporting log to identify someone who (1) tested positive for COVID-19 and (2) reported that test result in the relevant app. And, of course, a MAC address leading to a specific location is *not* PII in any case.

Second, Plaintiffs' fallback argument is that the non-PII logged by the EN System is logged "*alongside*" PII logged by *other* apps using the same crash-reporting log. Indeed, Plaintiffs acknowledge that RPIs and TEKs logged by the EN System do not contain PII. *See* FAC ¶¶ 27-29, 30, 39. But, Plaintiffs allege on information and belief that "other identifiers [such as the name of wireless networks, email address, device name] are logged on Android devices," though they do not specify by whom, when, or where. *Id.* ¶ 107. And, though Plaintiffs allege that Plaintiff Diaz's log file contained his email address and the name and address of his wireless network, *see id.* ¶ 138, the screenshots provided in the FAC do not support that claim, nor do Plaintiffs explain if *Google* logged that information. *See id.* ¶¶ 91–96. Indeed, Plaintiffs concede that Google instructs developers to refrain from logging of PII to crash-reporting logs. *Id.* ¶ 74.

Plaintiffs also vaguely suggest that device manufacturers and wireless network operators have access to PII elsewhere in their files, and so, for example, if they wanted to do the work, they could combine that information with the EN System's crash-reporting logs. *See id.* ¶ 99. But Plaintiffs provide no factual allegations showing how or whether EN System information is "formally linked" with such PII, or how or whether these disparate pieces of information are ever found in close proximity, particularly where the crash-reporting logs contain thousands of lines of technical, difficult-to-decipher entries. *See id.* ¶¶ 91–96; 102. Certainly, they don't allege that it's ever actually happened, or that Google enabled or encouraged it. Nor do they allege that anyone at Google has ever endeavored to combine data from different places in order to decipher an EN System user's identity, let alone link it to information about that individual's use of the EN System. None of the bases for Plaintiffs' alleged privacy harms stem from *Google's* conduct; at most, Plaintiffs complain that Google failed to stop a third party from logging PII to the same place the EN System uses for crash reporting purposes.

Third, the crash-reporting logs are ***temporary***. The logs contain temporary data that is maintained for a limited period of time for crash-reporting purposes. *See* FAC ¶¶ 57–59.

Plaintiffs' theory would require that a user reported a positive COVID test result, a different, unrelated application logged PII, and another third party accessed that log, identified the technical entries related to Exposure Notifications out of thousands of others, and pieced the available information together—all in the period of time before the data is overwritten.

Plaintiffs' theory of standing "relies on a highly attenuated chain of possibilities, [and] does not satisfy the requirement that threatened injury must be certainly impending." *Clapper*, 568 U.S. at 410. As the Supreme Court reiterated just recently, "[b]ecause no evidence in the record establishes a serious likelihood of disclosure, we cannot simply presume a material risk of concrete harm." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2212 (2021). Plaintiffs cannot establish that the "risk of harm is sufficiently imminent and substantial" as would be required for injunctive relief. *TransUnion LLC*, 141 S. Ct. at 2210. Even Plaintiffs do not allege that the EN System features they complain about still exist in the current EN System code. *FAC* ¶¶ 76–77; 86–88; 117–21. Accordingly, it is not reasonably likely that the risk of harm alleged in the FAC will materialize for Plaintiffs or any proposed class member.

ii. Plaintiffs fail to allege that they experienced actual harm.

Nor have Plaintiffs adequately alleged past harm that could support a claim for damages. Plaintiffs fail to allege that they experienced any harm at all, *i.e.*, that a third party or other bad actor accessed, disclosed, or misused their personal information as a result of the EN System. (Indeed, Plaintiff Bornmann does not even allege that he entered any information into the CA Notify app, or interacted with it in any way after activating it.) Nothing in the FAC suggests the conjectural harm Plaintiffs fear ever materialized, nor that other class members were even aware of or harmed by their exposure to the risk itself. *See TransUnion LLC*, 141 S. Ct. at 2211–12; FAC ¶ 98 (alleging that applications with access to system logs "***can***" easily associate the GAEN logs with the device owner's identity); FAC ¶ 105 ("entities in possession of log files . . . are also ***capable of*** associating RPIs with individuals); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012) ("the allegations that third parties can *potentially* associate LinkedIn identification numbers with information obtained from cookies and can de-anonymize a user's identity and browser history are speculative and relatively weak.").

Plaintiffs may argue that the simple act of a third party unknowingly having the ability to access a log that, with additional complicated work, could have made it easier for that third party to determine whether the user reported a positive COVID-19 test result to their EN app, constitutes sufficient disclosure for harm. The law disagrees. Even if a third party was able to access the crash-reporting logs, and even if they could decipher whose log it was, and even if they had in their possession the technical entries associated with the EN System app, those facts alone cannot constitute actionable disclosure. Indeed, courts have repeatedly held that in order to establish Article III standing to assert privacy claims under California law, it is not enough for Plaintiffs to plead that their personal information was *collected*; they must also allege that their personal information was *wrongfully disclosed*. That is because "[f]or a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party. . . . ***If no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated***." *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1088 (E.D. Cal. 2015) (finding no standing to bring claims of invasion of privacy or breach of confidentiality where the plaintiff failed to "allege[] facts from which a plausible inference could be drawn that [someone] has viewed his PII/PHI as a result of the Data Breach."); *see also TransUnion LLC*, 141, S. Ct., at 2210 ("The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm."); *Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776, 778 (9th Cir. 2018) (holding that the plaintiff failed to allege an injury for purposes of Article III where plaintiff did not allege that anyone viewed, stole, or otherwise used his private credit card information). The FAC falls short of alleging that any third party has associated "the data that GAEN logs with the device owner's identity," the FAC merely alleges that someone *could*. FAC ¶¶ 98, 105. That is not enough.

iii. Plaintiffs' alleged injury is not sufficiently particularized.

Plaintiffs also have not established that the alleged injury is "sufficiently particularized." *Jewel v. National Security Agency*, 673 F.3d 902, 909 (9th Cir. 2011). Plaintiffs' allegations relate only to Google's practices generally, and the allegations that third parties could *potentially* piece together EN System data with PII from other apps or device manufacturers are speculative. Nor

have Plaintiffs alleged that their personal information was disclosed to third parties as a result of Google's alleged practices. *See In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 977–78 (N.D. Cal. 2014); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011) (finding no credible, real, and immediate threat of harm where a digital service provider was alleged to have disclosed information to unauthorized third parties); *Yunker v. Pandora Media Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) (finding insufficient harm to confer standing where Pandora shared personal information without anonymizing it).

b. Plaintiffs' alleged injury is not fairly traceable.

Plaintiffs fail to plead facts sufficient to allege that their hypothetical injury is fairly traceable to the challenged conduct.[23] Plaintiffs do not assert the *EN System* logs PII to the crash-reporting logs—it doesn't. Plaintiffs instead allege that third parties could have logged PII in the same crash-reporting log despite the fact that, as Plaintiffs concede, doing so is against Google's recommended best practices. *Compare* FAC ¶¶ 69 (admonishing app developers that logs are a "shared resource" that should not include PII ") *and* 74 (Google "instructs" app developers that they "must not log any [PII]") *with* 107–08 (claiming on information and belief that crash-reporting logs include email addresses) *and* 137 (claiming Plaintiff Diaz's logs "***already***" contained his e-mail address because of a different app's logging practices). Plaintiffs' theory then requires that other bad actors could find those needles in a haystack within the crash-reporting logs at the exact time they are in the logs, and then discern their meaning and piece them together to attempt to learn something about a person's COVID-19 test result. Because Google's alleged liability hinges on the acts of third parties, the alleged harm isn't fairly traceable to Google's conduct. *See Clapper*, 568 U.S. at 413. Indeed, if *no* app ran afoul of Google's best practices, then the entire theory underlying the FAC, would collapse. *See* FAC ¶¶ 74; 107–10 (alleging that the

[23] Plaintiffs do claim that the EN System shouldn't log MAC addresses because a third party could, through some work, determine a location for that MAC address. That is not the same as PII, as discussed *supra* Part III.C.1.a.i.

crash-reporting logs used by the EN System may contain PII that was *logged by others against Google's guidance*). Standing law forbids making litigants responsible for the acts of third parties.

c. Plaintiffs' alleged injury is not redressable.

Plaintiffs cannot show that their alleged injury is likely to be redressed by a favorable decision. Plaintiffs request that the Court enjoin Google from "(1) continuing to copy Plaintiffs' and Class Members' personal and medical information to the system logs on Android devices and from continuing to allow unauthorized parties access to Plaintiffs' and Class Members' personal and medical information in the system logs"; "(2) continuing to collect Plaintiffs' and Class Members' personal and medical information in the system logs"; and "(3) requiring Google to ensure that all personal and medical information acquired, created, or otherwise obtained from the system logs is destroyed." FAC at 35–36. Because Plaintiffs concede that the logging no longer exists in the updated code, prospective injunctive relief will not redress Plaintiffs' claimed harm. FAC ¶¶ 76, 77, 79, 86-88. Moreover, the temporary nature of the logged data additionally demonstrates that the alleged *historical* features of the EN System could not present any harm going forward.

As for past harms, Plaintiffs request "actual and/or statutory and/or special and/or incidental damages and restitution" as well as "punitive damages and exemplary damages." FAC at 36. But, as discussed previously, because Plaintiffs do not allege any facts from which it could reasonably be inferred that anyone has linked their identities to a decision to report a positive COVID-19 test result,, as described above, they have not suffered a cognizable harm and therefore could not be entitled to any form of relief for past harm under any of the asserted privacy claims.

Plaintiffs therefore lack Article III standing. This Court should not "abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors." *Clapper*, 568 U.S. at 414. The FAC should be dismissed for lack of Article III standing under Federal Rule of Civil Procedure 12(b)(1).

IV. RULE 12(B)(6) MOTION TO DISMISS

A. Legal Standard

A motion to dismiss for failure to state a claim under Rule 12(b)(6) tests the legal sufficiency of the complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). To survive a motion to dismiss under Rule 12(b)(6), a plaintiff must plead facts showing that his right to relief rises above "the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," and pleadings that are "no more than conclusions, are not entitled to the assumption of truth." *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009). A court need not accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

Dismissal without leave to amend is appropriate if "amendment would be futile." *Carrico v. City & Cnty. of San Francisco*, 656 F.3d 1002, 1008 (9th Cir. 2011). An amendment is futile when "no set of facts can be proved under the amendment to the pleadings that would constitute a valid and sufficient claim or defense." *Miller v. Rykoff-Sexton, Inc.*, 845 F.2d 209, 214 (9th Cir. 1988).

B. Argument

The fundamental defect in the FAC is that it cannot reasonably be inferred that anyone has ever exploited the features Plaintiffs complain about in the EN System to decipher a user's identity and link it to technical entries buried in a system log that reflect their decision to report a positive COVID-19 test result. As previously discussed, this central defect leaves Plaintiffs' theory of liability riddled with problems of logic, law, and fact. Because Plaintiffs' allegations cannot support the crux of their FAC, Plaintiffs' claims fail under Rule 12(b)(6).

1. Plaintiffs fail to state a claim for public disclosure of private facts because there was no public disclosure.

For a common-law public disclosure of private facts claim, a plaintiff must allege disclosure to the public "at large." *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1062 (N.D. Cal. 2014). In *Opperman*, the court dismissed the public disclosure claim where plaintiffs alleged that

their phone address books were transmitted in an unencrypted manner, or over public Wi-Fi, "making [them] publicly available to third parties as well as service providers." *Opperman*, 87 F. Supp. 3d at 1062. The court reasoned that the plaintiffs failed to meet the disclosure requirement because "[w]hile Plaintiffs alleged that their information could have been intercepted by third parties, they do not allege that any interception occurred, nor do they allege that it was 'substantially certain' that their address books would become 'public knowledge.'" *Id.* In the instant case, Plaintiffs have alleged even fewer facts that could lead to an inference of public disclosure "at large" of "private facts."

First, the data logged by the EN System to the system logs in question are not "private facts" because they do not reveal any personally identifying information about the user. *See, e.g.*, *Taus v. Loftus*, 40 Cal. 4th 683, 717–18 (2007) (stating that private facts constitute sufficiently sensitive or intimate details of plaintiffs' lives). Plaintiffs allege that the logging of RPIs, the logging of a report of a positive COVID-19 test result, or the logging of transmission ofTEKs (all non-PII) *could be* viewed by unauthorized entities, but that alone is not enough; Plaintiffs not only fail plausibly to allege anyone has ever done this, but they fail to allege that any of these unnamed entities took steps to decipher the user's identity using other sources of information (*not* from the design of the EN System apps themselves) in order to infer the COVID-19 diagnosis of a particular individual.

Second, there is no allegation of public disclosure. Plaintiffs allege that disclosure of their system log information would have been only to entities that were provided access to the crash-reporting log by device manufacturers, rather than to the public at large. *See* FAC ¶ 98. Plaintiffs have not alleged that members of the general public outside this limited number of app developers or device manufacturers would even be able to access, view, or piece together crash-reporting information to reveal a person's "private facts," or that it is "substantially certain" members of the general public would do so. Simply put, even if the alleged disclosure to a select group of "privileged" entities happened, and even if someone employed by those entities then took additional steps to link a user's identity to their report of a COVID-19 test result, even that does not constitute *public* disclosure of private facts.

Third, access to the list of TEKs associated with a positive diagnosis is restricted to public health authorities. Plaintiffs baldly assert that the list of TEKs associated with a positive diagnosis are "publicly available," "published for anyone to access." FAC ¶¶ 39, 89, 106. But a TEK is, by itself, meaningless. Indeed, the EN System was designed so that TEKs are not linked back to a user, as Plaintiffs concede. The public listing of TEKs do not even figure into Plaintiffs' attenuated chain of events that would have to unfold in order for a bad actor to link a user's identity to a report of a COVID-19 test result. To the extent Plaintiffs claim that *anyone* can access the TEK list, that is beside the point, as a TEK by itself is meaningless.

Indeed, to allege that their personal information was publicly available, Plaintiffs would have had to allege an improbable series of events: that members of the general public (i) knew what these MAC addresses, crash-reporting logs, RPIs, and TEKs are; (ii) retrieved them from users' devices; (iii) cross-referenced a TEK list; and then (iv) matched them up to randomized RPIs; (v) deciphered the user's identity to attempt to learn information about a specific individual; and (vi) released that information to the public. The several breaks in causation in that speculative chain alone are enough to doom Plaintiffs' claims at the pleading stage.

2. Plaintiffs fail to state a claim for intrusion upon seclusion or invasion of privacy because the alleged intrusion was not intentional or highly offensive.

A claim for intrusion upon seclusion under California common law requires a showing that "(1) a defendant 'intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]' and (2) the intrusion 'occur[red] in a manner highly offensive to a reasonable person." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). "The intrusion must be intentional." *Varnado v. Midland Funding LLC*, 43 F. Supp. 3d 985, 992 (N.D. Cal. 2014). "Effective consent negates an intrusion upon seclusion claim." *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016).

A plaintiff alleging an invasion of privacy under the California Constitution must show that "(1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious. . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet*

Tracking Litig., 956 F.3d at 601. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37 (1994). "The California Constitution . . . set[s] a high bar for an invasion of privacy claim." *Low*, 900 F. Supp. 2d at 1025. "Even negligent conduct that leads to theft of highly personal information, including social security numbers, does not 'approach [the] standard' of actionable conduct under the California Constitution." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012); *see also Razuki v. Caliber Home Loans, Inc.*, No. 17-cv-1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. June 7, 2018) (dismissing California Constitution invasion of privacy claim because plaintiff's allegations "don't suggest the type of intentional, egregious privacy invasion contemplated" by case law).

Because the tests for intrusion upon seclusion and invasion of privacy are so similar, "courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 601.

First, Plaintiffs have not alleged facts showing that any intrusion occurred; that is, that third-party entities or members of the general public gained unwanted access to their personal information. Plaintiffs present a theory of how their privacy could have been violated, but "it is not clear that anyone has actually done so, or what information, precisely, these third parties have obtained." *Low*, 900 F. Supp. 2d at 1025; *see also In re Zoom Video Comms. Inc. Privacy Litig.*, No. 20-CV-02155-LHK, 2021 WL 930623, at *15 (N.D. Cal. Mar. 11, 2021) (dismissing plaintiffs' invasion of privacy claim because "[p]laintiffs fail to allege that Zoom actually shared *their* personal data with third parties"); *cf. McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1035 (N.D. Cal. 2019) ("Plaintiffs state in detail what data was secretly collected, how the collection was done, and how the harvested data was used.").

Second, Plaintiffs have not pled any facts showing that, if any intrusion occurred, such intrusion was intentional. The facts alleged in Plaintiffs' FAC show that the EN System was set up during a time of international crisis for the purpose of providing a benefit to society in the midst of

a global pandemic. It was created not for profit, but with the goal of enabling contact tracing in a privacy-protective manner. Indeed, the outside sources provided by Plaintiffs (Google requests judicial notice of a few of them), indicate that Google set the EN System up with every intention of ensuring that *no* intrusion or invasion of privacy would occur.[24] The screenshot of Google's instructions to Android developers included in the FAC show that Google instructed developers to "not log any Personally Identifiable information (PII) as part of normal operation."[25] Plaintiffs also allege that, only a few weeks after Google allegedly became aware of the allegations in this case, Google "began to . . . roll[] out patch fixes."[26] The facts alleged in Plaintiffs' FAC, taken as true, not only fail to show intent to invade privacy; they affirmatively demonstrate the opposite. *See Razuki*, 2018 WL 2761818, at *2 (holding that "[plaintiff's] allegations don't suggest the type of intentional, egregious privacy invasion contemplated" by California case law where plaintiff alleged defendant failed to protect his personal data by choosing to implement low-budget security measures).

Third, any intrusion into data that is not personally identifiable cannot be highly offensive because Plaintiffs, through enabling exposure notifications and activating the CA Notify app, understand that RPIs and TEKs will be stored on their own devices and broadcast and exchanged with other participating devices. The potential access to or disclosure of randomized RPIs, entries reflecting upload of TEKs, and technical activity names contained in the crash-reporting logs by an app developer, or a device manufacturer, would not be highly offensive where Plaintiffs understand that RPIs will be broadcast from their phones to nearby devices and their identity could potentially be guessed by a party who receives their exposure notifications if they had only a limited number of contacts on a given day.[27] *See Opperman*, 87 F. Supp. 3d at 1059 ("the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant.").

[24] *See* Google's RJN Exs. 1–3.
[25] FAC ¶ 74.
[26] FAC ¶ 117.
[27] *See e.g.* MD Covid Alert Privacy Policy, Maryland Department of Health CovidLINK, https://covidlink.maryland.gov/content/mdcovidalert/privacy-policy/ (last visited June 26, 2021).

The allegation that third parties such as phone manufacturers (who themselves have their own terms of use with their customers) were able to access crash-reporting logs, without more, hardly constitutes an "egregious breach of social norms" or a "serious invasion" of a privacy interest. *See Low*, 900 F. Supp. 2d at 1025 (holding that Plaintiffs failed to state a claim for invasion of privacy where LinkedIn allegedly disclosed to third parties the numeric code associated with a user and the URL of the profile page used, and that there was no evidence third parties de-anonymized this data to obtain personal information); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (holding that the alleged disclosure of unique device identifier number, personal data, and geolocation information from Plaintiffs' Apple devices did not constitute an egregious breach of privacy under the California Constitution); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 987–88 (N.D. Cal. 2014) (holding that plaintiffs' allegations that user data was disclosed to third-party developers contrary to Google's own policies failed to meet the high bar for intrusion upon seclusion). The hypothetical access by third parties of crash-reporting log information logged by the EN System app, which alone cannot be used to identify an individual or their COVID-19 diagnosis, falls far below the high standard necessary to state a claim for intrusion upon seclusion or invasion of privacy.

3. Plaintiffs fail to state a claim under the CMIA because Google is not a provider of health care and Plaintiffs' medical information has not been collected, disclosed, or viewed.

The CMIA, Cal. Civ. Code §§ 56 *et seq.*, prohibits a provider of health care from disclosing, either purposefully or negligently, medical information without the patient's consent. Cal. Civ. Code §§ 56.10, 56.101. Plaintiffs allege that Google violated sections 56.10(a), 56.10(d), 56.10(e), 56.26(a), and 56.101(a) of the CMIA.

a. Google is not a provider of health care under the CMIA.

The CMIA's definition of "provider of health care" includes the following:

> (a) Any business **organized for the purpose of maintaining medical information**, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care . . . .

> (b) Any business that offers software or hardware to consumers, including a mobile application or other related device that is **designed to maintain medical information**, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care . . . .

Cal. Civ. Code §§ 56.06(a)–(b).

Plaintiffs have not alleged facts sufficient to establish that Google is a provider of health care as defined by the CMIA. Plaintiffs simply make the following conclusory statements:

> Google is a "Provider of Health Care" under Cal. Civ. Code § 56.06(a) because it is a business that created GAEN for use in mobile devices using Google's Android operating system for the purpose of maintaining medical information in order to make the information available to an individual for management and diagnosis of potential exposure to COVID-19.
>
> Google is a "Provider of Health Care" under Cal. Civ. Code § 56.06(a) because Google is a business organized for the purpose, among others, of maintaining medical information in order to make the information available to individuals and providers of health care.
>
> Google is a "Provider of Health Care" under Cal. Civ. Code § 56.06(b) because through GAEN, Google offers software designed to maintain information about whether a user has tested positive for COVID-19 and whether a user has been exposed to COVID-19, in order to make the information available to the user and to California public health authorities, at the request of the user and of California public health authorities, for the treatment and management of COVID-19.

FAC ¶¶ 179–81.

First, Plaintiffs cannot allege that Google is a "business organized for the **purpose** of maintaining medical information" as required by Civ. Code § 56.06(a). Indeed, courts applying the CMIA have cabined its application to traditional providers of health care, such as hospitals. *See, e.g.*, *Regents of University of California v. Superior Court*, 163 Cal. Rptr. 3d 205 (Ct. App. 2013) (applying the CMIA to the University of California at Los Angeles health system); *Sutter Health v. Superior Court*, 174 Cal. Rtpr. 3d 653 (Ct. App. 2014) (applying the CMIA to Sutter Health); *Eisenhower Medical Center v. Superior Court*, 172 Cal. Rptr. 3d 165 (Ct. App. 2014) (applying the CMIA to Eisenhower Medical Center). Plaintiffs' FAC alleges that "Google's

business model involves and derives revenue from collecting, aggregating, and analyzing many different kinds of data in large quantities for commercial purposes, including advertising." FAC ¶ 179. Taking Plaintiffs' allegation as true, Google's purpose involves commercial data uses such as advertising, not "maintaining medical information." Civ. Code § 56.06(a). The Court should decline to adopt Plaintiffs' novel and expansive interpretation of the applicability of the CMIA.[28]

Second, Plaintiffs have failed to allege facts sufficient to establish that the Google was "organized for the purpose of maintaining **medical information**" or that the EN System was "designed to collect and maintain its users' **medical information**," as required by Civ. Code §§ 56.06(a) and 56.06(b). The CMIA defines the term "medical information" as follows:

> **any individually identifiable information**, in electronic or physical form, in possession of or derived from a provider of health care . . . **regarding a patient's medical history, mental or physical condition, or treatment.** 'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, **alone or in combination with other publicly available information, reveals the individual's identity.**

Civ. Code § 56.05. The CMIA's definition of "medical information" has two necessary elements: (1) "individually identifiable information," i.e., information that "alone or in combination with other publicly available information, reveals the individual's identity," and (2) information regarding "a patient's medical history, mental or physical condition, or treatment." *See* Civ. Code § 56.05. Any one element, by itself, is insufficient: "This definition does not encompass demographic or numeric information that does not reveal medical history, diagnosis, or care." *Eisenhower Med. Ctr.*, 172 Cal. Rptr. 3d at 169. In other words, release of individually identifiable information in and of itself (such as the fact that a patient visited a certain doctor or clinic) is

[28] Plaintiffs allege that Google is a provider of health care, in part, because "historically Google offered a product called Google Health." FAC ¶ 180. The Google Health service to which Plaintiffs refer was discontinued in 2012. *Google Health, the company's newest product area, has ballooned to more than 500 employees*, CNBC, Feb. 11, 2020, https://www.cnbc.com/2020/02/11/google-health-has-more-than-500-employees.html. "Google Health" now refers to teams working within Google, rather than a service or application. *Id.*

insufficient to violate the statute. *Id.* at 170. "[T]he mere fact that a person is or was a patient is not accorded the same level of privacy as more specific information about his medical history." *Id.*

The purpose of the EN System, as Plaintiffs acknowledge, was to *avoid* maintenance of "individually identifiable information" coupled with information about an individual's "medical history, diagnosis, or care." Plaintiffs allege "Google represents that GAEN does not share a user's identity" and "Google has represented [that GAEN d]oesn't collect personally identifiable information." FAC ¶¶ 44, 47. As Plaintiffs' allegations demonstrate, the EN System was not organized for the purpose of maintaining medical information; quite the opposite, it was designed to enable health authorities to privately conduct contact tracing and to delete such information from phones after 14 days. Additionally, a document Plaintiffs rely upon in their FAC provides that "Google will not receive identifying information about the user, device location data, or information about any other devices the user has been in proximity of." FAC n. 17.[29]

Third, Plaintiffs have failed to allege facts sufficient to establish that the EN System was created "in order to make the [medical] information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual." Cal. Civ. Code §§ 56.06(a), 56.06(b). Civ. Code §§ 56.06(a) and 56.06(b) were added to the CMIA in 2013 to clarify that personal health records, such as those offered as an application by a commercial vendor of personal health service software to allow an individual to monitor and manage his or her own medical information, are also subject to CMIA protections. A.B. 658, Assem. Com. on Jud., at 4–5 (Ca. 2013). The legislative history makes clear that the amendments were ***not*** intended to apply to "all medical information, broadly construed, that is created by the individual," such as pedometer data generated by a fitness application. Rather, the intent was to "protect medical information that originated with medical professionals, whether providers, insurers, administrators, or other contractors who held a person's medical information." *Id.* Contact-tracing applications using the EN System, akin to the fitness applications that collect

[29] Google's RJN Ex. 3.

information that does not originate with medical professionals, are the types of applications to which the CMIA was ***not*** intended to apply.

Plaintiffs have stated that the purpose of the EN System was to make medical information (which, as previously discussed, requires individually identifiable information) available to "the user and to California public health authorities, at the request of the user and of California public health authorities, for the treatment and management of COVID-19." FAC ¶ 181.[30] The very documents that Plaintiffs reference in their FAC, and of which Google requests judicial notice, contradict this statement.[31] As previously discussed, the EN System was organized specifically *not* to collect or maintain individually identifiable information. Additionally, the EN System was created for the purpose of warning *other* users of potential COVID-19 exposure, not for "the diagnosis and treatment of the individual" where "individual" refers to the user of the app. The EN System cannot diagnose an individual with COVID, nor treat a COVID-positive individual. Nor is the reporting of a positive test result a medical diagnosis. Because Plaintiffs fail to allege facts sufficient to establish that Google is a "provider of health care," Plaintiffs cannot state a claim for violation of the CMIA.

b. The app does not collect medical information.

Even assuming that Google meets the definition of "health care provider," any information collected by the EN System does not meet the definition of medical information; thus, Plaintiffs cannot state a claim under the CMIA.

The randomized identifiers—RPIs, TEKs, and MAC addresses—are random strings of characters and numbers, periodically regenerated so as to minimize the likelihood that they would be used to identify an individual. Plaintiffs have not alleged that these pieces of non-PII contained

[30] Paragraph 181 of the FAC appears to assume that "California public health authorities" would be considered "provider[s] of health care" under the CMIA; however, Plaintiffs do not provide any facts to explain how "California public health authorities" meet any of the CMIA's definitions of "provider of health care," including as defined under Sections 56.05(m), 56.06(a), or 56.06(b). *See, e.g.*, Cal. Civ. Code § 56.06(a) ("Any business organized for the purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care").

[31] *See* Google's RJN Exs. 1–3 (discussing the intent of the EN System to avoid collection of individually identifying information, such as user identity).

in the crash-reporting log alone can be used to identify an individual, nor that the EN System ties any PII to the report of a positive COVID-19 test result.

As previously discussed, the CMIA's definition of "medical information" contains two necessary elements: (1) individually identifiable information and (2) information about medical history, diagnosis, or care. *See, e.g.*, *Eisenhower*, 172 Cal. Rptr. 3d. at 168–69; Civ. Code § 56.05. The randomized identifiers and exposure notifications alone cannot be used to identify an individual, nor have Plaintiffs alleged that anyone has used these randomized identifiers or exposure notifications in such a way as to actually identify individuals.[32]

c. Plaintiffs are not "patients" of Google.

Plaintiffs allege that Google violated sections 56.10(a), 56.10(d), 56.10(e), 56.26(a), and 56.101(a) of the CMIA, all of which prohibit a provider of health care from disclosing a **patient's** medical information. Plaintiffs' claims fail for the additional reason that Plaintiffs are not "patients" of Google. The CMIA defines "patients" as "any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains." Civ. Code § 56.05(k). Though the term "health care services" is not defined in the CMIA, "logic dictates that in order for a health care provider to gather medical information about a person, the provider must have dealt with the person at some level and performed professional services of some type." *Pettus v. Cole*, 57 Cal. Rptr. 2d 46, 64 (Ct. App. 1996). "Health care services" include professional services such as medical examinations, pre-employment physical examinations, and psychiatric evaluations. *Id.* at 64–65. The provision of an application that allows users to receive exposure notifications and report COVID test results is far from the type of "health care services" contemplated by the statute; the EN System does not

[32] As to Plaintiff Bornmann, the CMIA claim fails on the additional ground that he did not provide any information to the app. Plaintiffs do not allege that he provided information about his medical history, diagnosis, or care to the app, nor that he reported a COVID-positive test result through the app. Without that, Plaintiff Bornmann cannot plead a violation of the CMIA because none of his medical information would have been available to be disclosed. Simply downloading and activating the app, without more, does not provide the app with any information about the user's medical history, diagnosis, or care. Thus, even assuming that personally identifiable information was disclosed (as explained above, it was not), Plaintiff Bornmann has not pled that he reported a COVID test result through the app and thus cannot plead a violation of the CMIA.

diagnose, examine, or treat users of the app. Plaintiffs therefore cannot assert a CMIA claim because they are not "patients" within the definition of the CMIA.

d. Plaintiffs have not pled that disclosure of medical information occurred under section 56.10.

Civil Code section 56.10 prohibits health care providers from "disclos[ing]" medical information. The word "disclose" requires a plaintiff to plead an "affirmative communicative act" by the defendant, more than just making medical information accessible via the Internet. *Stasi v. Inmediata Health Group Corp.*, No. 19cv2353 JM (LL), 2020 WL 6799437, at *14 (S.D. Cal. Nov. 19, 2020). Rather, a plaintiff must allege that the defendant intentionally posted their information, or did some other affirmative act with intent to communicate that information. *Id.*

Plaintiffs have not alleged that Google took an "affirmative communicative act" with intent to communicate their medical information, as required by Section 56.10. As previously discussed, the facts alleged in the FAC lead to the opposite conclusion—that any medical information, if disclosed, was not done so intentionally. Therefore, Plaintiffs cannot plead a violation of Section 56.10 of the CMIA.

e. Plaintiffs have not alleged that the medical information was viewed by an unauthorized person, as required by sections 56.101 and 56.36.

Section 56.101 of the CMIA provides that any health care provider "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." In order to state a claim under Sections 56.101 and 56.36 of the CMIA, a plaintiff must allege that the medical information was viewed by an unauthorized person. *Sutter Health*, 174 Cal. Rptr. 3d at 655. If no unauthorized person has viewed the medical information, no confidentiality breach has occurred. *Id.* at 661.

Plaintiffs have not alleged that the medical information was viewed by an unauthorized person, as required by Sections 56.101 and 56.36. *Id.* at 661. In *Sutter Health*, a computer with medical information stored on it was stolen. However, there was no allegation that the thief—or anyone else—had viewed the medical information on the hard drive. The court concluded that, even if Sutter had been negligent in storing the medical information on the computer, without an

allegation that an unauthorized person had viewed the records (and that confidentiality was breached), there is no negligent release in violation of Sections 56.101 and 56.36 of the CMIA, and there is no remedy, even for nominal damages. *Sutter* 174 Cal. Rptr. 3d at 661–62. In the instant case, Plaintiffs allege that their non-personally identifiable system log information was exposed to third parties and that certain third parties may be able to match this non-PII to individuals. That is completely speculative. There is no allegation that anyone has viewed and matched any COVID-19 diagnosis or exposure to any individual. Plaintiffs cannot state a claim for a violation of Sections 56.101 and 56.36 of the CMIA.

V. AMENDMENT WOULD BE FUTILE

Plaintiffs should not be given leave to amend their FAC where, as here, amendment would be futile. Plaintiffs cannot carry their burden of establishing subject-matter jurisdiction. Plaintiffs have already amended their Complaint once. The FAC still fails to plead any facts to support Plaintiffs' allegation that any bad actor has matched any PII to any positive COVID-19 test result, as required to state a claim for the alleged violations of their privacy rights. For these reasons, Plaintiffs' FAC should be dismissed without leave to amend.

VI. CONCLUSION

For the foregoing reasons, Google respectfully requests that the Court dismiss the FAC with prejudice.

WILLKIE FARR & GALLAGHER LLP

Date: August 25, 2021

By: */s/ Benedict Y. Hur*
Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Tiffany Lin

Attorneys for Defendant
Google LLC